CRY 2025

Laboratoire #3

20-05-2025

Préambule

- Ce laboratoire demande de résoudre différents challenges basés sur la cryptographie asymétrique. Chaque étudiant doit rendre un rapport **individuel** avec ses propres solutions ainsi que son code. Les façons d'arriver à la solution sont libres mais doivent être expliquées dans le rapport.
- Vous pouvez par contre discuter ensemble pendant que vous résolvez les problèmes. Essayez de ne pas spoiler !
- Voici une liste de fonctions qui pourraient vous être utiles en python :
  - dans le module pycryptodome [1] : `Crypto.PublicKey.RSA`, `Crypto.Cipher.PKCS1_OAEP`, `Crypto.Hash`, `Crypto.Util.Padding` et `Crypto.Cipher.AES`.
  - dans le module base64 : `base64.b64encode()`, `base64.b64decode()`
- Toutes les données **binaires** sont en **base64**. N'oubliez pas de les décoder avant de les utiliser.
- Certains exercices peuvent contenir des mots tirés aléatoirement. Ne vous en offensez pas et googlez-les à vos risques et périls.
- Vous trouverez vos entrées personnalisées dans le zip `nom_prenom.zip` sur cyberlearn.
- Le **rapport** et votre **code** doivent être rendus dans un zip sur cyberlearn avant le **01.06 à minuit**.
- Il se peut que j'annonce des erreurs sur cyberlearn/teams.

1 "Encryption" (2 pts)

Le fichier `encryption.sage` contient un algorithme de chiffrement asymétrique.

1. Dessinez un schéma correspondant à cet algorithme. (0.2 pts)
2. Donnez une description mathématique du chiffrement **et du déchiffrement correspondant**. (0.2 pts)

   Indice : Regardez bien ce que fait la fonction `pad`.
3. Implémentez le déchiffrement. Testez votre code et montrez votre test dans votre rapport. (0.3 pts)
4. On suppose que les quatre racines carrées d'un texte chiffré ont fuité lors du déchiffrement. Vous trouverez dans votre fichier de paramètres la clef publique n, un message clair m, son texte chiffré correspondant c, les quatre racines carrées de c. Vous trouverez aussi un texte chiffré "challenge" chiffré avec la même clef. Décryptez-le. Donnez dans votre rapport le message récupéré ainsi qu'une explication mathématique expliquant votre attaque. (1 pt)

   Indice : Visualisez ces racines dans $\mathbb{Z}_p \times \mathbb{Z}_q$ et effectuez des opérations sur ces dernières afin d'obtenir un multiple de p ou de q.
5. Sur quel problème difficile est basé cette construction ? (0.1 pt)
6. A quoi sert la redondance dans la construction (variable `REDUNDANCY`) ? (0.2 pts)

1. https://pycryptodome.readthedocs.io

2 Courbes Elliptiques (2 pts)

Vous trouverez dans le fichier `elliptic.sage` un algorithme de chiffrement asymétrique basé sur les courbes elliptiques.

1. Dessinez un schéma correspondant à cet algorithme. (0.2 pts)
2. Donnez une description mathématique du chiffrement **et du déchiffrement correspondant**. (0.2 pts)
3. Implémentez le déchiffrement. Testez votre code et montrez votre test dans votre rapport. (0.3 pts)
4. Il y a un problème dans cet algorithme. Lequel ? (0.1 pts)
5. Cassez la construction. Vous trouverez dans votre fichier de paramètres la clef publique et un texte chiffré complet (avec nonce et tag). Tout est en base64. Donnez dans votre rapport le message récupéré ainsi qu'une explication de votre attaque. (1 pt)
6. Corrigez l'erreur dans la construction. (0.2 pts)

3 RSA (1 pt)

Vous trouverez dans le fichier `rsa.sage` une implémentation de textbook RSA.

1. Implémentez le déchiffrement. Testez votre code et montrez votre test dans votre rapport. (0.5 pts)
2. Cassez la construction. Vous trouverez dans votre fichier de paramètres la clef publique et un texte chiffré complet. Le texte chiffré est en base64. Donnez dans votre rapport le message récupéré ainsi qu'une explication de votre attaque. (0.5 pts)